
KYRUS

Pragmatic Approach to Breaking Mobile Apps

Rich Smith
rich@kyr.us

- Who are Kyrus? - http://kyr.us
- Washington DC, New York, Chicago, San Antonio
- ‘The Cyber Security Skunkworks’
- Vulnerability Research
- Reverse Engineering
- Forensics
- Custom Software Development

Introduction

- Talk is focussed on application security not OS security (See Dino's talk)
  - What Apps do wrong despite the OS
  - Bugs vs Flaws
- The principles are general
- Rationale is aimed at Enterprises & SMBs

Aims

- Rapidly validate a mobile App against a specific threat model
- End up with a quantifiable set of risks that can be mitigated, or knowingly accepted
- You won't stop the mobile device tide, just try understand your risks

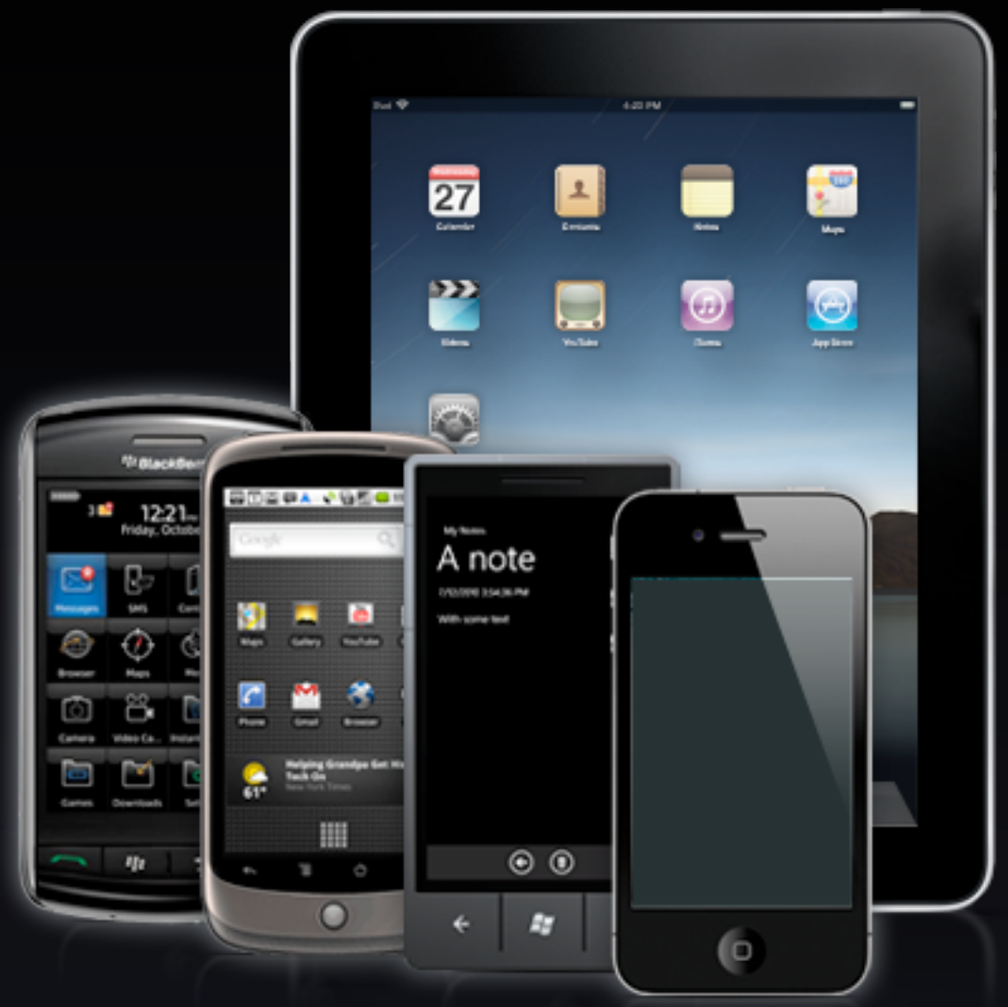
KYRUS

Avoid

- Blindly believing vendor security claims
- Your company ending up on the front page of Morgunblaðið

The Changing Landscape

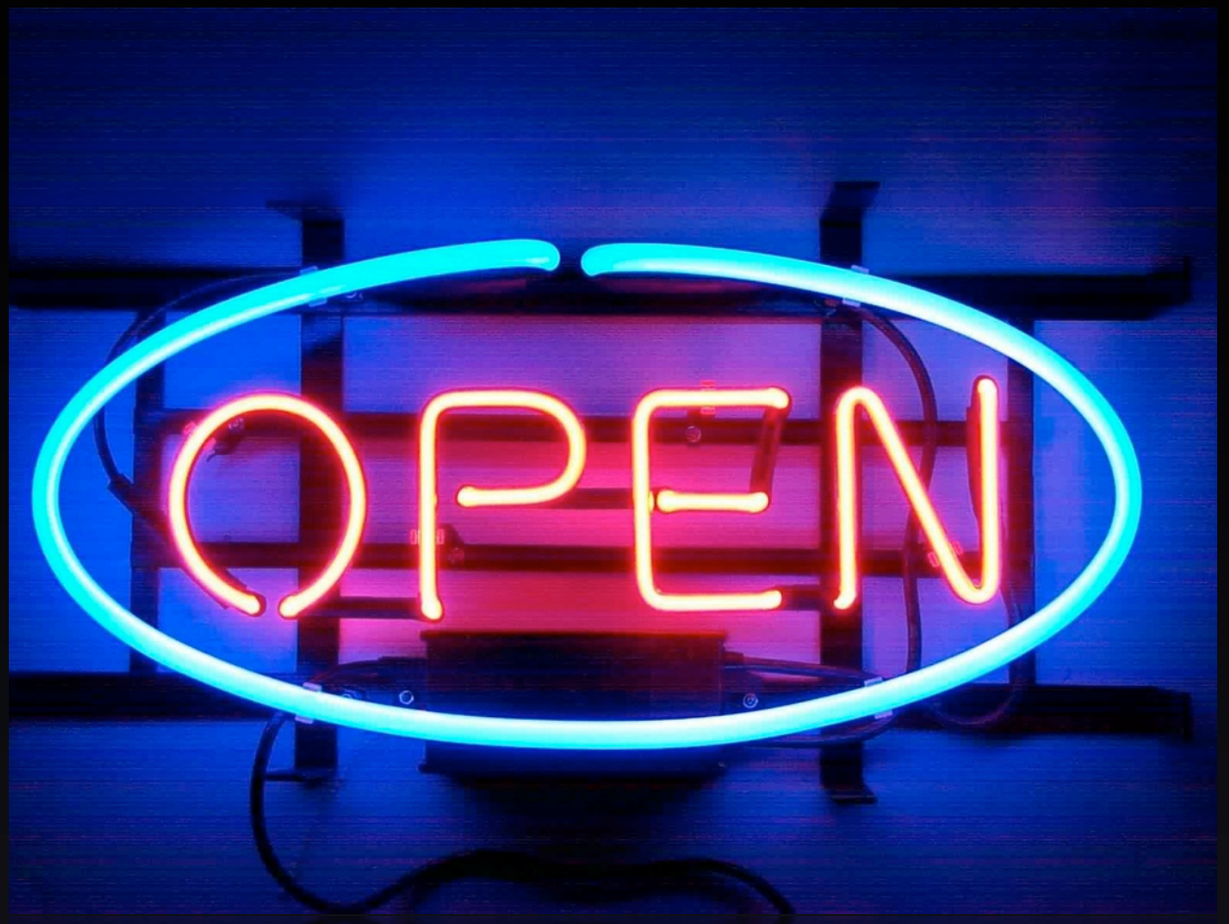
Mobile devices are at the centre of many current tech trends



KYRUS

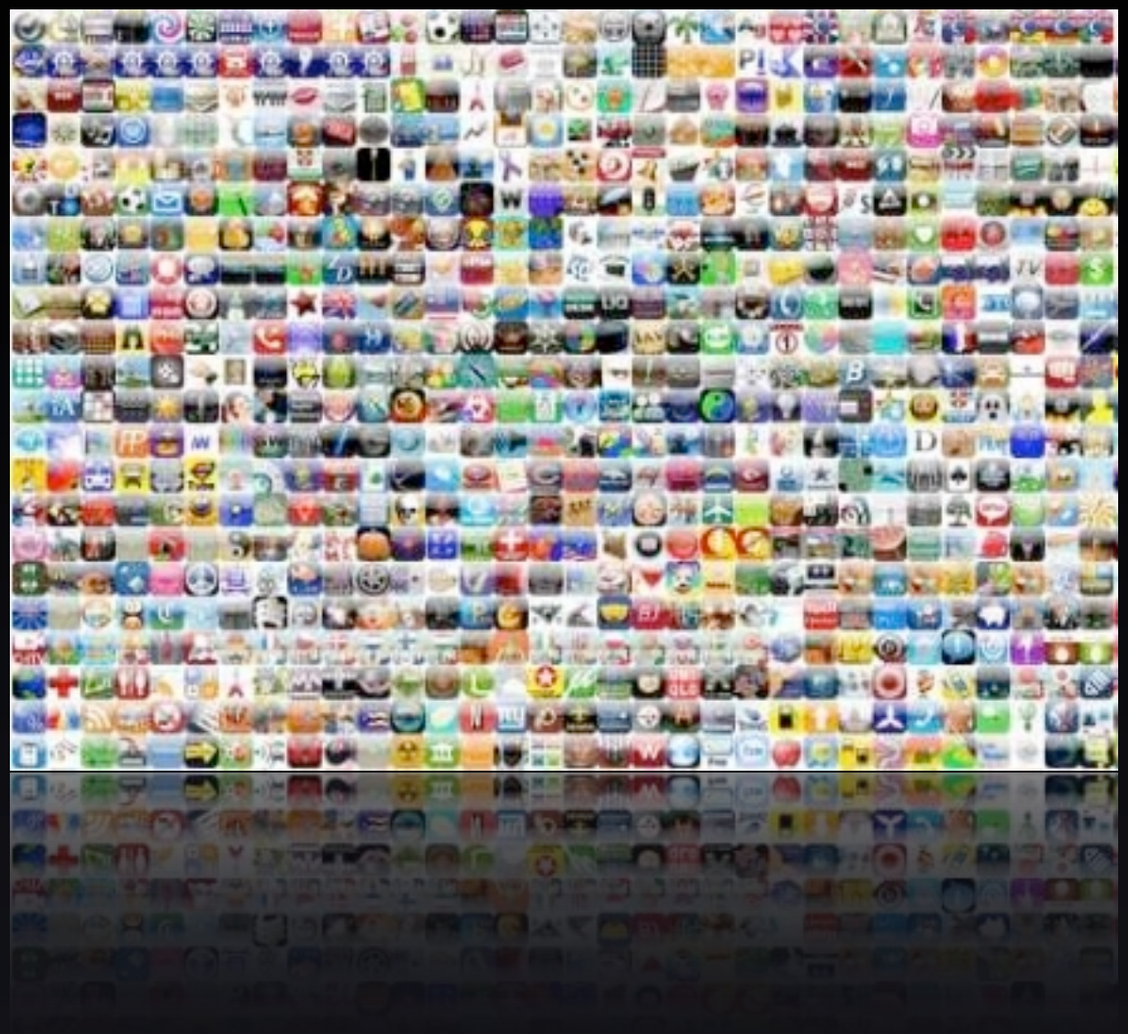
The Cloud

KYRUS



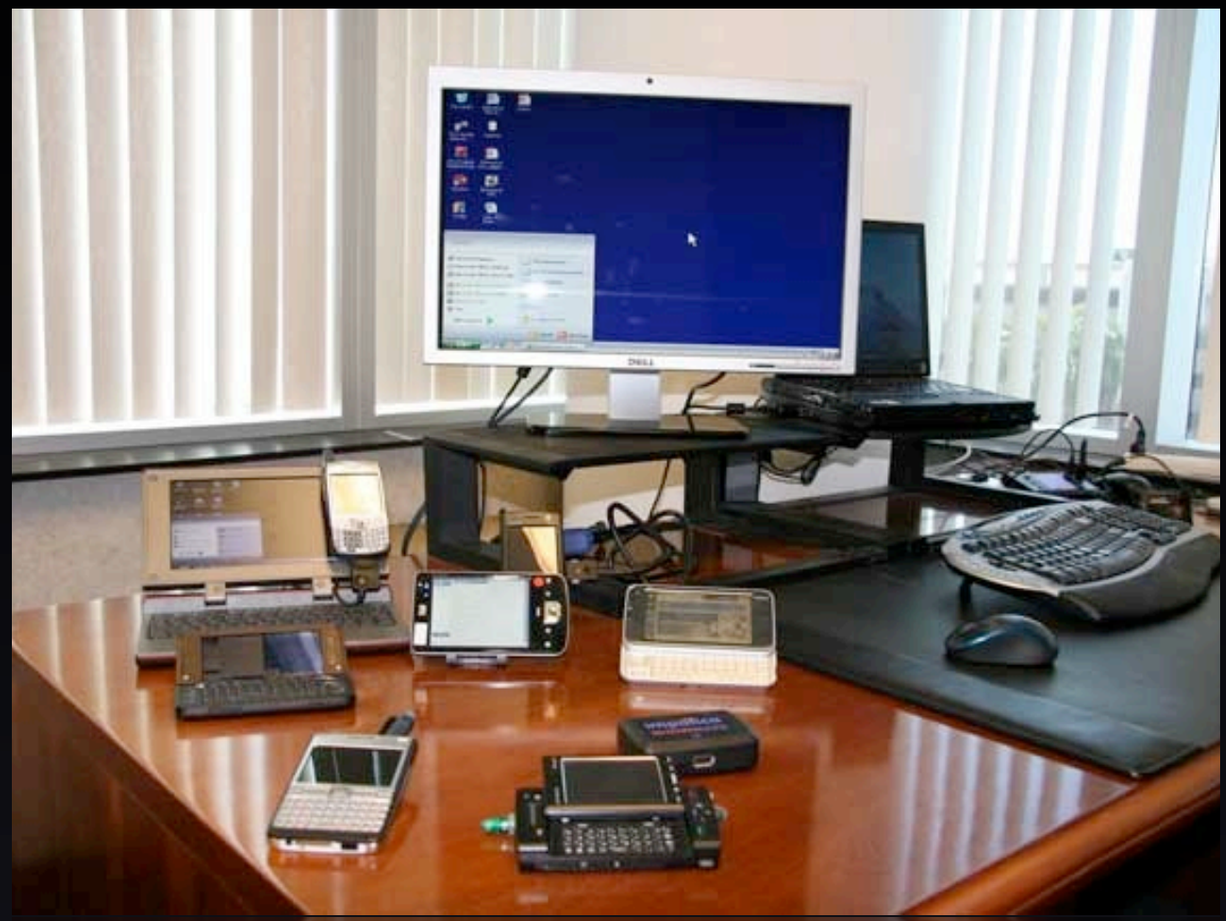
Open APIs

KYRUS



App Stores

KYRUS



BYOD - Bring Your Own Device

KYRUS

Mobile Landscape

- While these trends don't create a *requirement* for mobile device usage....
- ....they increase the *pressure* for them to be used everywhere

KYRUS

Mobile Landscape

- This pressure is coming from senior business people
  - They handle the most sensitive data
  - They see security as getting in the way
  - They wanted it yesterday .....

KYRUS

...so JUST APPROVE IT ALREADY!

KYRUS

The Real World™

- You will be asked to approve increasing numbers of mobile apps in 2012
- You won't have as long as you want to assess them

KYRUS

The Real World™

- You will be assessing Apps from small & start up vendors
- They won't have security as a core skill or priority, time to market wins all

KYRUS

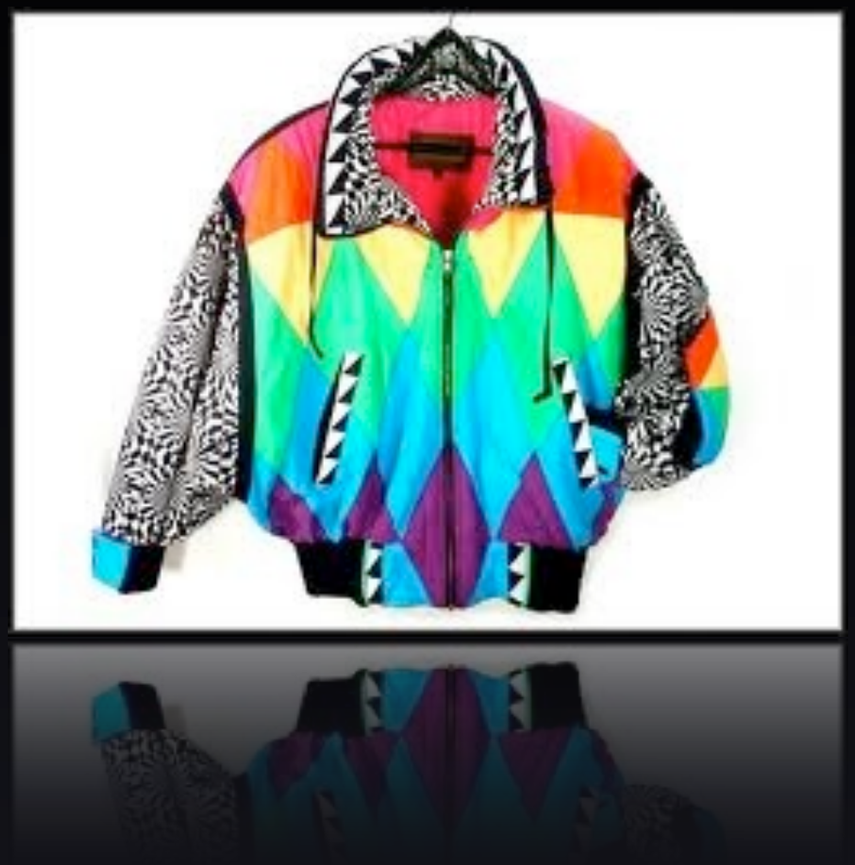
The Real World™

- You will need to prioritise high risk, low hanging fruit
- You won't have time to reverse out every function

KYRUS

The Real World™

- You will see the same mistakes again, and again and again .....



You will feel like you doing security back in the 90's again!

KYRUS

Pragmatic Assessment

- Rapidly assess an App with focus on the areas of highest risk for the given usage
- Take a threat centric view of the App
- Produce a set of well understood risks that you can mitigate or accept

KYRUS

Total Cost of 0wnership

- Think in terms of 'TC0'
- How much effort will it cost an attacker to take advantage of the latest mobile must-have App ?

KYRUS

Primary Risks for this App

Sensitive Data Loss	Loss / Theft of device Loss amplification
Device as Facilitator	Does possession of the device provide advantage for backend attack?
Loss Detection	Do you know if the data is compromised?

KYRUS

Threat Centric View

- How is the user authenticated
  - Enrolment, forgotten password..
- How does the device operate offline
- How is data at rest secured
- How does it use the OS services

?

Spurningar

rich@kyr.us


KYRUS